Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	

VERIZON REPLY IN SUPPORT OF USTELECOM'S PETITION FOR RECONSIDERATION AND REQUEST FOR CLARIFICATION

The Commission should protect consumers from unwanted and illegal robocalls by granting the relief requested in USTelecom's Petition for Reconsideration and Request for Clarification[1] of the blocking notification provisions in the Fourth Report and Order.[2] Absent modification, the rules requiring instantaneous notification to calling parties will give robocallers a new attack vector to bypass blocking tools, raise substantial security concerns, and deter service providers from offering more robust robocall blocking services to consumers in the first place. While Verizon favors ensuring that legal, authenticated callers have access to information about how their calls are treated, the rules should be recalibrated to protect consumers at least as much as they protect robocallers.

I. THE RULES WOULD HARM CONSUMERS BY GIVING ROBOCALLERS A TOOL TO BYPASS BLOCKING AND TO LAUNCH MALICOUS ATTACKS ON CONSUMERS AND NETWORKS

The Petition echoes concerns pointed out on the record about the dangers of mandating ubiquitous instantaneous free notifications for every call a service provider blocks: robocallers

[1] Petition for Reconsideration and Request for Clarification of USTelecom – The Broadband Association, filed in CG Docket No. 17-59 (May 6, 2021) ("*Petition*").

[2] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, Fourth Report and Order, 35 FCC Rcd 15221 (2020) ("*Order*").

will have a new ecosystem-wide tool to test and then bypass blocking tools and to engage in other malicious conduct.[3] Consumers will be harmed by a notification regime that provides *all* callers – regardless of whether or not they submit to best practices or are authenticated as legal – with instantaneous call-by-call feedback. At a minimum, the instantaneous notification mandate promises to increase the efficiency with which robocallers – both legal and illegal – can detect blocking and swap new phone numbers into the "calling party" field to avoid being blocked. And more pernicious potential use cases for the release codes are also lurking. For example, fraudsters could use them to identify which numbers have been assigned to human beings, thus enabling them to efficiently target lists of consumers as opposed to their more common current practice of inefficiently "carpet bombing" entire swaths of numbers. Innovative malicious actors may also choose to launch denial of service attacks or employ other techniques to "punish" consumers that choose to make use of service providers' opt-in or opt-out blocking tools.

The 608 release code specification confirms these concerns about potential unintended consequences. It emphasizes that service providers sending the release code must be "mindful" to whom they are sending it because "the caller, now alerted that an intermediary is automatically rejecting their call, may change their call behavior to defeat call-blocking systems."[4] Specifically, because of the risk of giving bad actors new attack vectors to harm service providers' consumers or networks, the 608 specification recommends that service providers not send any Call-Info with a release code unless the calling party has been authenticated.[5] And it notes that if service providers include their contact information in the

[3] *Petition* at 6-7.

[4] *See* Internet Engineering Task Force, RFC 8688, A Session Initiation Protocol (SIP) Response Code for Rejected Calls (Dec. 2019), https://tools.ietf.org/html/rfc8688 at 15-16 ("*SIP Code 608 Specification*").

[5] *Id.*

release code, malicious actors may use that attack vector to "launch an attack" on the service provider."[6] Both the 607 and 608 specifications identify the need to work through various other security challenges associated with the potential use of the standards (none of which has been addressed by any industry standards body), ranging from harms caused by malicious actors spoofing release codes to "man in the middle" attacks.[7]

Parties opposing the Petition argue that the Commission has already rejected these concerns, citing its statement that "the potential harm from providing notifications to bad actors is more than offset by the significant benefit to legitimate callers."[8] But that analysis has several flaws. First, neither the Order nor the parties opposing the Petition acknowledge the need to address the security concerns that the 607 and 608 specifications identify as necessary prior to implementation. Second, the Order does not define the terms "legitimate caller" or "bad actor" and does set forth the criteria calling parties should be expected to meet in order to receive notifications. While most enterprises making high-volume calls to their customers make good faith efforts to avoid irritating those consumers, and thus are appropriately seeking blocking transparency to correct false positives, unfortunately even some legal callers routinely take action to bypass blocking – even when the blocking algorithms are working as intended – when they detect that their calls may have triggered blocking algorithms.[9] Given that even *legal*

[6] *Id.*

[7] *Id.*; Internet Engineering Task Force, RFC 8197, A SIP Code for Unwanted Calls (July 2017), https://tools.ietf.org/html/rfc8197 at 6 ("*SIP Code 607 Specification*").

[8] ABA Partial Opposition at 7-8 (quoting *Order* at para. 54); INCOMPAS Opposition at 5 (quoting *Order* at para. 54).

[9] One commenter in CG Docket No. 17-59 filed a patent application for the practice of cycling through a pool of available telephone numbers in order to bypass blocking and labeling as soon as it is detected through various means. *See* Calling Party Number Selection for Outbound Telephone Calls to Mitigate Robocalling Processing Impacts, U.S. Patent No. 10,205,699 B1 (Feb. 12, 2019).

robocallers are already monitoring outbound calls for blocking and taking action to bypass that blocking, it follows that both legal and illegal robocallers would leverage the release code feedback to more effectively and efficiently engage in such bypassing, thus increasing the flood of robocalls consumers receive and undermining tools to limit unwanted calls.

The Order incorrectly cites two calling parties' comments for its conclusion that "bad actors" are already capable of changing their phone numbers in order to bypass blocking.[10] But those commenters support a finding that the release code mandate would indeed make it easier and cheaper for all callers – legal and illegal – to bypass blocking. Noble Systems notes that some "contact centers" (presumably talking about legal ones) *already* monitor their contact rates in order to determine if their calls may be being blocked, and notes that illegal callers already spoof to avoid blocking.[11] But it ignores that service providers are working hard to address the spoofing problem (an arms race that the release code mandate would make harder for service providers and their analytics engines to fight) and does not rebut the fact that mandating release codes would make it easier and efficient for *all* calling parties to avoid blocking. Indeed, NAFCU explains that it supports a notification mandate because its members "do not have the resources" to track busy signals in order to detect blocking, confirming that free standardized notifications would improve all robocallers' ability to efficiently monitor and bypass blocking.[12]

[10] *See Order* at para. 54 (citing Comments of Noble Systems Corporation (Aug. 31, 2020) and Comments of NAFCU (Jan. 29, 2020).

[11] Noble Systems Corporation Comments at 20.

[12] NAFCU Comments at 3. The VON Coalition argues that the bypassing concern is unpersuasive because there are other ways to "reverse engineer" which calls are blocked, noting that callers can discover what calls are blocked "by opening an account with that terminating provider and making calls to that account to see whether they're passed to the dialed number." VON Coalition Comments at 4. That might be true, but it is not reasonable to conclude that such a bypassing operation could be carried out as effectively or efficiently as relying on standardized release codes to detect when blocking algorithms begin to identify a calling number as unwanted.

It is thus impossible for opponents of the Petition to seriously argue that such bypassing practices – which are already being done in real life – will not become more ubiquitous and efficient if the rules are permitted to go into effect absent modification. And it would be bad policy to shrug off the risk that the release codes could be used for the malicious purposes discussed above, in the Petition, and in the 607 and 608 specifications themselves. Instead, the Commission should make clear that "legitimate" callers (however it defines that term) should follow best practices that include cleaning up their calling practices if their calls are identified as unwanted by blocking algorithms working as intended, and agreeing not to attempt to bypass legitimate blocking using release codes or any other type of feedback. And to the extent it leaves in place a release code mandate in some form, it should make clear that service providers have discretion – as proposed in the 608 Specification – to not send release codes where they are unable to authenticate the identity of the caller.[13]

II. THE COMMISSION SHOULD NOT PRESCRIBE TECHNICAL REQUIREMENTS THAT ARE UNVETTED AND/OR NOT ACCOUNTED FOR IN THE STANDARDS

A. The 607 and 608 Specifications Are Raw Protocols That Cannot Be Safely and Responsibly Implemented Until Appropriate Standards and Best Practices Are in Place.

As the Petition points out, the Commission erred in prescribing a set of actions based on an unfinished standard that has not been vetted in the IP-NNI task force. A policy leveraging standards bodies' outputs should, like the Commission did with STIR/SHAKEN, rely on standards vetted by industry. But Section 64.1200(k)(9) instead prescribes a set of network practices, including prescriptive protocol mapping obligations applying to every intermediate

[13] *Cf. id.* at 16 (explaining that because of the security and bypassing concerns, service providers "may wish to configure their response to only include Call-Info header field for INVITE, or other signed initiating methods, that pass validation by STIR).

service provider in the call path (*see* subpart (iii)), despite the fact that the IP-NNI task force has only begun to explore the network resiliency, reliability, and security issues associated with implementing these protocols.[14]

Letting the industry standards process play out is particularly important here because the rules repurpose the 607 and 608 codes in ways that are inconsistent with the contents of the RFCs. Release code 607 proposes that a terminating carrier would use release codes generated from called parties for the *pro-consumer* purpose of using that data to develop call blocking algorithms to protect those customers from future unwanted calls[15]; it does not contemplate sending release codes upstream all the way to originating service providers in order to inform them about blocks, as mandated by Section 64.1200(k)(9). And the 608 RFC specifically contemplates that terminating service providers should not tip off calling parties about their calls being blocked unless those parties have been authenticated,[16] which also conflicts with Section 64.1200(k)(9). The Commission should reconsider its decision to mandate uses for protocols not contemplated – let alone vetted – by industry standards bodies or by the protocols themselves.

B. If the Commission Leaves in Place a Release Code Mandate, It Should Reject Requests to Expand it to Include a Complex Cryptographically-Signed "jCARD."

If the Commission decides to continue the course of mandating instantaneous notifications via release codes, despite the risks that policy poses, it should reject proposals from two commenters to foist a granular "jCARD" obligation onto service providers[17] that would take

[14] *Petition* at 3-6.

[15] *SIP Code 607 Specification* at 2 (proposing that the terminating carrier can use rejections by called parties "as input to a heuristic algorithm for determining future call treatment).

[16] *See SIP Code 608 Specification* at 15-16.

[17] *See* ABA Opposition at 6-7; INCOMPAS Opposition at 9-11.

years to develop and implement. Section 64.1200(k)(9) requires only that blocking service providers "return…an appropriate response code" to the originator of the call. The Commission did not and should not prescribe the policy that service providers may put in place with respect to different options consistent with the protocols.

Including a jCARD would involve cryptographically signing each release code with the blocking service provider's contact information and the reason the call was rejected, which would essentially require the entire industry to duplicate – in reverse – the STIR/SHAKEN regime that we have just spent years developing and implementing. In addition to developing the jCARD standards themselves, the infrastructure required for jCARD would need to include standing up a governance authority, policy administrator, and certificate authority. That would impose massive costs and administrative burdens on service providers that would deter them from continuing or beginning to offer blocking services to their customers. The proponents of a jCARD mandate do not even attempt to address the cost recovery issues associated with their proposal, a serious oversight given that they are the cost causers and (along with fraudulent robocallers) the beneficiaries.

III. THE NOTIFICATION OBLIGATIONS RISK UNDOING THE EXTRAORDINARY CONSUMER BENEFITS CREATED BY THE COMMISSION'S GREEN LIGHTS TO BLOCK MORE AGGRESSIVELY

A. Consumer Privacy and Other Policy Considerations Require Clarifying that the Scope of Any Notification Mandate Does Not Extend to Consumer-Directed Blocking.

The Petition urges the Commission to clarify that any notification expectation should extend only to situations where a service provider blocks calls based on analytics designed to

identify unwanted or illegal robocalls.[18] That is crucial because whatever notification regime the Commission settles on should not in any way tip off calling parties to attempts to block and stop telephone denial of service attacks, to "Do Not Originate" blocks, or to instances where a consumer has given specific blocking instructions. Providing notice in these situations could cause substantial unintended consequences, including hampering attempts to stop denial of service attacks and ignoring privacy expectations of consumers who have chosen to block certain calls.

B. Asymmetrically Foisting Harmful Notification Obligations on Service Providers Would Drive Consumers to Use Device-Based and Other Third Party Blocking.

Verizon and other service providers have a strong interest in protecting our customers from unwanted robocalls, and thus are actively deploying and improving call blocking and labeling services.[19] The Commission should contemplate that robocall blocking and labeling, which is still in its infancy, will continue to evolve, including as other stakeholders in the ecosystem increasingly work to protect consumers. For example, Verizon last year announced a partnership with Apple in which we assist Apple to deploy device-based blocking to consumers. And numerous providers of blocking apps also compete for customers based on protecting them from unwanted robocalls. While the Commission should encourage third parties to innovate to protect consumers, it should not handicap service providers with harmful asymmetrical obligations that do not apply to others. Doing so would strand a substantial amount of investment and innovation that we have brought to bear to address the robocall problem and

[18] *Petition*, Section III.

[19] *See, e.g.*, Letter from Christopher D. Oatway, Associate General Counsel, Federal Regulatory and Legal Affairs, Verizon, to G. Patrick Webre, Consumer & Governmental Affairs Bureau, FCC, WC Docket No. 17-97 at 2 (Apr. 30, 2021).

thereby harm consumers.

***

Respectfully submitted,

William H. Johnson
Of Counsel

Gregory M. Romano
Christopher D. Oatway
1300 I Street, N.W.
Suite 500 West
Washington, DC 20005
(202) 515-2470

Attorneys for Verizon and Verizon Wireless

June 14, 2021